

Secure cloud computations: Description of (fully)homomorphic ciphers within the P-adic model of encryption

Andrei Khrennikov and Ekaterina Yurova
International Center for Mathematical Modelling
in Physics and Cognitive Sciences
Linnaeus University, Växjö, S-35195, Sweden
Andrei.Khrennikov@lnu.se

March 25, 2016

Abstract

In this paper we consider the description of homomorphic and fully homomorphic ciphers in the p -adic model of encryption. This model describes a wide class of ciphers, but certainly not all. Homomorphic and fully homomorphic ciphers are used to ensure the credibility of remote computing, including cloud technology. The model describes all homomorphic ciphers with respect to arithmetic and coordinate-wise logical operations in the ring of p -adic integers \mathbb{Z}_p . We show that there are no fully homomorphic ciphers for each pair of the considered set of arithmetic and coordinate-wise logical operations on \mathbb{Z}_p . We formulate the problem of constructing a fully homomorphic cipher as follows. We consider a homomorphic cipher with respect to operation $"*"$ on \mathbb{Z}_p . Then, we describe the complete set of operations $"G"$, for which the cipher is homomorphic. As a result, we construct a fully homomorphic cipher with respect to the operations $"*"$ and $"G"$. We give a description of all operations $"G"$, for which we obtain fully homomorphic ciphers with respect to the operations $"+"$ and $"G"$ from the homomorphic cipher constructed with respect to the operation $"+"$. We also present examples of such "new" operations.

keywords: p -adics, p -adic functions, homomorphic ciphers, fully homomorphic ciphers, dynamical systems, 1-Lipschitz

1 Introduction

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers, [1]. Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. A cryptosystem that supports arbitrary computation on ciphertexts is known as fully homomorphic encryption (FHE), [2]. The existence of an efficient and fully homomorphic cryptosystem would have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing, [3].

A brief review of the known homomorphic encryption algorithms is presented in [14]. Examples of implemented fully homomorphic ciphers exist - see, for example, [11], [12], [13], [16].¹

The general idea of homomorphic (and fully homomorphic) encryption is as follows (for example, [23], [24]). Suppose we have a set of data M . The operations $g_1 : M \times M \rightarrow M$, $g_2 : M \times M \rightarrow M$ are defined on the set M (for homomorphic encryption only one operation is required). It is necessary to find the value of an expression $W(d_1, \dots, d_n)$, which is defined through the operations g_1 and g_2 on the data $d_1, \dots, d_n \in M$. By analogy with the formulas of Boolean algebra, the expression W can be considered as a formula in the basis g_1 and g_2 (for more details see section 5). If the calculation of the formula W is performed remotely (for example, using cloud services), then the user sends the data d_1, \dots, d_n to an untrusted environment (for example, to the cloud server). After that, the result of the computing returns to the user. In this case, the user's data become open.

We understand a cipher as a family of bijective transformations of the set M , where each transformation is identified by a certain parameter – the encryption key. Suppose we have a cipher with the following property with respect to the operations g_1, g_2 . For every transformation of encryption f_a , where a is a key, the following relations $f_a(g_1(x, y)) = g_1(f_a(x), f_a(y))$ and $f_a(g_2(x, y)) = g_2(f_a(x), f_a(y))$, $x, y \in M$ hold. Then, $f_a(W(d_1, \dots, d_n)) = W(f_a(d_1), \dots, f_a(d_n))$. This means that the remote computations are performed on encrypted data $f_a(d_1), \dots, f_a(d_n)$ and the result of calculations $W(d_1, \dots, d_n)$ is obtained in encrypted form $f_a(W)$. That is, only the user

¹However, there are some drawbacks in these schemes. For example, in the scheme of C. Gentry, the size of the ciphertext and computational complexity for encryption and decryption grows exponentially depending on the number of operations on the plaintext. In [16], to compute the encrypted value of the product of plaintexts, it is necessary to use one of the plain texts explicitly.

has access to the data d_1, \dots, d_n . In general, this approach provides complete trust in remote computing.

In this paper, we consider the description of all homomorphic and fully homomorphic ciphers for the p -adic model of encryption with respect to a given set of operations, namely, arithmetic ("+" and ".") and coordinate-wise logical ("XOR" and "AND"), defined on the set of p -adic integers \mathbb{Z}_p . This model involves the automata implementation of encryption functions on the set of words in the alphabet $\{0, 1, \dots, p-1\}$.

We start our paper by recalling definitions that are related to the p -adic analysis, as well as introducing the necessary notations.

In section 2 we describe the p -adic model of encryption. Moreover, we show that the problem of description of homomorphic (fully homomorphic) ciphers is reduced to the description of the measure-preserving 1-Lipschitz functions $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, which defines a homomorphism with respect to a given operation (relatively, to a given pair of operations) on \mathbb{Z}_p .

In the p -adic model of encryption the Theorems 3.1 and 3.3 describe all homomorphic ciphers with respect to arithmetic operations "+", "." and coordinate-wise logical operations "XOR" and "AND" on \mathbb{Z}_p . Based on these theorems, Proposition 4.1 shows that a fully homomorphic cipher does not exist with respect to all possible pairwise combinations of the operations from the set $\{ "+", "\cdot", \text{"XOR"}, \text{"AND"} \}$. In this regard, in section 4 we discuss the following possibility of constructing a fully homomorphic cipher within the p -adic model of encryption. Let us choose a homomorphic cipher with respect to a given operation "*" (for example, we take the operation "+" as "*"). Then we set on \mathbb{Z}_p the new operation $G : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ such that a given cipher is homomorphic. Operation G can be set as a convergent in the p -adic metric power series on \mathbb{Z}_p . In this case, the homomorphic cipher is a fully homomorphic cipher with respect to the operations "*" and " G ". Of course, the new operation " G " will not have such properties as associativity, commutativity, etc. In Proposition 4.2 we give a description of all operations " G ", for which we obtain fully homomorphic ciphers with respect to the operations "+" and " G " from the homomorphic cipher with respect to the operation "+". At the end of the section 4, we present examples of such "new" operations.

In section 5 we discuss the possibility of remote computing security by using a fully homomorphic encryption on particularly chosen operations for a given computational procedure (that is, the formulas implemented by a computer program).

1.1 P -adic numbers

For any prime number p the p -adic norm $|\cdot|_p$ is defined on \mathbb{Q} in the following way. For every nonzero integer n let $\text{ord}_p(n)$ be the highest power of p which divides n . Then we define $|n|_p = p^{-\text{ord}_p(n)}$, $|0|_p = 0$ and $|\frac{n}{m}|_p = p^{-\text{ord}_p(n) + \text{ord}_p(m)}$.

The completion of \mathbb{Q} with respect to the p -adic metric $\rho_p(x, y) = |x - y|_p$ is called the field of p -adic numbers \mathbb{Q}_p . The metric ρ_p satisfies the so-called strong triangle inequality $|x \pm y|_p \leq \max(|x|_p, |y|_p)$. The set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is called the set of p -adic integers.

Hereinafter, we will consider only the p -adic integers. Every $x \in \mathbb{Z}_p$ can be expanded in canonical form, namely, in the form of a series that converges for the p -adic norm: $x = x_0 + px_1 + \dots + p^k x_k + \dots$, $x_k \in \{0, 1, \dots, p-1\}, k \geq 0$.

Let $a \in \mathbb{Z}_p$ and r be positive integers. The set $B_{p^{-r}}(a) = \{x \in \mathbb{Z}_p : |x - a|_p \leq p^{-r}\} = a + p^r \mathbb{Z}_p$ is a ball of radius p^{-r} with center a .

1.2 P -adic functions

In this paper, we consider functions $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, which satisfy the Lipschitz condition with constant 1 (i.e. 1-Lipschitz functions). Recall that $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is a 1-Lipschitz function if

$$|f(x) - f(y)|_p \leq |x - y|_p, \quad \text{for all } x, y \in \mathbb{Z}_p.$$

This condition is equivalent to the following: $x \equiv y \pmod{p^k}$ follows $f(x) \equiv f(y) \pmod{p^k}$ for all $k \geq 1$.

For all $k \geq 1$ a 1-Lipschitz transformation $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ of the reduced mapping modulo p^k is

$$f_{k-1} : \mathbb{Z}/p^k\mathbb{Z} \rightarrow \mathbb{Z}/p^k\mathbb{Z}, \quad z \mapsto f(z) \pmod{p^k}. \quad (1.1)$$

Mapping f_{k-1} is well defined (the f_{k-1} does not depend on the choice of representative in the ball $z + p^k \mathbb{Z}_p$).

1.2.1 Van der Put series

P -adic functions can be represented in the form of the van der Put series. The van der Put series is defined in the following way. Let $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be a continuous function. Then there exists a unique sequence of p -adic coefficients B_0, B_1, B_2, \dots such that

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) \quad (1.2)$$

for all $x \in \mathbb{Z}_p$. Here the characteristic function $\chi(m, x)$ is given by

$$\chi(m, x) = \begin{cases} 1, & \text{if } |x - m|_p \leq p^{-n}; \\ 0, & \text{otherwise,} \end{cases}$$

where $n = 0$ if $m = 0$, and n is uniquely defined by the inequality $p^{n-1} \leq m \leq p^n - 1$ otherwise (see Schikhof's book [10] for detailed presentation of the theory of the van der Put series). The number n in the definition of $\chi(m, x)$ has a very natural meaning. It is just the number of digits in a base- p expansion of $m \in \mathbb{N}_0$. Then

$$\lfloor \log_p m \rfloor = (\text{the number of digits in a base-}p \text{ expansion for } m) - 1,$$

therefore $n = \lfloor \log_p m \rfloor + 1$ for all $m \in \mathbb{N}_0$ and $\lfloor \log_p 0 \rfloor = 0$ (recall that $\lfloor \alpha \rfloor$ denotes the integral part of α).

The coefficients B_m are related to the values of the function f in the following way. Let $m = m_0 + \dots + m_{n-2}p^{n-2} + m_{n-1}p^{n-1}$, $m_j \in \{0, \dots, p-1\}$, $j = 0, 1, \dots, n-1$ and $m_{n-1} \neq 0$, then

$$B_m = \begin{cases} f(m) - f(m - m_{n-1}p^{n-1}), & \text{if } m \geq p; \\ f(m), & \text{otherwise.} \end{cases} \quad (1.3)$$

1-Lipschitz functions $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ in terms of the van der Put series were described in [10]. We follow Theorem 3.1 [22] as a convenience for further study. In this theorem, the function f presented via the van der Put series is 1-Lipschitz if and only if $|B_m|_p \leq p^{-\lfloor \log_p m \rfloor}$ for all $m \geq 0$. Assuming $B_m = p^{\lfloor \log_p m \rfloor} b_m$, we find that the function f is 1-Lipschitz if and only if it can be represented as

$$f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} b_m \chi(m, x) \quad (1.4)$$

for suitable $b_m \in \mathbb{Z}_p$, $m \geq 0$.

1.2.2 Coordinate representation of 1-Lipschitz functions

In this section we describe a coordinate representation of p -adic functions, see, for example, [21].

We recall that any p -adic integer (as an element of the ring \mathbb{Z}_p) can be expanded into the series:

$$x = x_0 + p x_1 + \dots + p^k x_k + \dots, \quad x_j \in \{0, 1, \dots, p-1\}.$$

Let us denote

$$\begin{aligned}(x)_k &= x_0 + x_1p + \dots + x_{k-1}p^{k-1}, \quad k \geq 1, \\ [x]_k &= (x_0, x_1, \dots, x_{k-1}), \quad k \geq 1.\end{aligned}\tag{1.5}$$

Let functions $\delta_k(x)$, $k = 0, 1, 2, \dots$ be k -th digit in a base- p expansion of the number $x \in \mathbb{Z}_p$, i.e. $\delta_k: \mathbb{Z}_p \rightarrow \{0, 1, \dots, p-1\}$, $\delta_k(x) = x_k$.

Any map $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ can be represented in the form:

$$f(x) = \delta_0(f(x)) + p\delta_1(f(x)) + \dots + p^k\delta_k(f(x)) + \dots \tag{1.6}$$

According to Proposition 3.33 in [9], f is a 1-Lipschitz function if and only if for every $k \geq 1$ the k -th coordinate function $\delta_k(f(x))$ does not depend on $\delta_{k+s}(x)$ for all $s \geq 1$, i.e. $\delta_k(f(x + p^{k+1}\mathbb{Z}_p)) = \delta_k(f(x))$ for all $x \in \{0, 1, \dots, p^{k+1} - 1\}$.

Taking into account notation 1.5 for $k \geq 0$, we consider the following functions of p -valued logic

$$\varphi_k: \underbrace{\{0, \dots, p-1\} \times \dots \times \{0, \dots, p-1\}}_{k+1} \rightarrow \{0, \dots, p-1\},$$

and $\varphi_k: [x]_{k+1} \mapsto \delta_k(f(x))$.

Then any 1-Lipschitz function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ can be represented as

$$f(x) = f(x_0 + \dots + p^k x_k + \dots) = \sum_{k=0}^{\infty} p^k \varphi_k(x_0, \dots, x_k) = \sum_{k=0}^{\infty} p^k \varphi_k([x]_{k+1}). \tag{1.7}$$

The function $\varphi_k(x_0, \dots, x_k)$ can be defined by its sub-functions obtained by fixing the first k variables (x_0, \dots, x_{k-1}) . By 1.5, the sub-function of the function $\varphi_k(x_0, \dots, x_k)$ which is obtained by fixing the variables $x_0 = a_0, \dots, x_{k-1} = a_{k-1}$, $a_i \in \{0, \dots, p-1\}$, is denoted by $\varphi_{k,[a]_k}$, where $a = a_0 + pa_1 + \dots + p^{k-1}a_{k-1}$. In these notations, the function $\varphi_k(x_0, \dots, x_k)$ can be represented as

$$\varphi_k(x_0, \dots, x_k) = \sum_{a=0}^{p^k-1} I_{[a]_k}(x_0, \dots, x_{k-1}) \varphi_{k,[a]_k}(x_k), \tag{1.8}$$

where $I_{[a]_k}$ is a characteristic function, i.e.

$$I_{[a]_k}(x_0, \dots, x_{k-1}) = \begin{cases} 1, & \text{if } (x_0, \dots, x_{k-1}) = [a]_k; \\ 0, & \text{otherwise.} \end{cases}$$

Thus, we can rewrite the 1-Lipschitz function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ as

$$f(x) = \sum_{k=0}^{\infty} p^k \varphi_k(x_0, \dots, x_k) = \varphi_0 + \sum_{k=1}^{\infty} p^k \sum_{a=0}^{p^k-1} I_{[a]_k}([x]_{k-1}) \varphi_{k,[a]_k}(x_k). \quad (1.9)$$

We call the relation 1.9 the coordinate representation of 1-Lipschitz function f .

Any function φ_k can be given by a polynomial of the ring of $(k+1)$ -variate polynomials $(\mathbb{Z}/p\mathbb{Z})[x_0, \dots, x_k]$, with coefficients from the residue ring $\mathbb{Z}/p\mathbb{Z}$, whose degree in each variable is at most $p-1$. In other words, φ_k is defined as an element of a factor-ring $(\mathbb{Z}/p\mathbb{Z})[x_0, \dots, x_k]$ modulo an ideal generated by all polynomials $x_i^p - x_i$, $i = 0, 1, \dots, k$.

The function φ_k can be represented in the form (expansion by the leading variable x_k):

$$\varphi_k(x_0, \dots, x_k) = x_k^{p-1} \alpha_{p-1}(x_0, \dots, x_{k-1}) + \dots + \alpha_0(x_0, \dots, x_{k-1}),$$

where $\alpha_i(x_0, \dots, x_{k-1}) \in (\mathbb{Z}/p\mathbb{Z})[x_0, \dots, x_{k-1}]$, $i = 0, 1, \dots, p-1$. In particular,

$$\varphi_{k,[a]_k} = x_k^{p-1} \alpha_{p-1}([a]_k) + \dots + \alpha_0([a]_k)$$

is a polynomial from $(\mathbb{Z}/p\mathbb{Z})[x_k]$ ($\alpha_i([a]_k) \in \mathbb{Z}/p\mathbb{Z}$, $i = 0, 1, \dots, p-1$).

Thus, the coordinate functions $\varphi_{k,[a]_k}$, φ_0 can be considered as a function of p -valued logic and as a transformation of the ring $\mathbb{Z}/p\mathbb{Z}$.

1.3 P -adic dynamics

Dynamical system theory studies trajectories (orbits), i.e. sequences of iterations:

$$x_0, x_1 = f(x_0), \dots, x_{i+1} = f(x_i) = f^{(i+1)}(x_0), \dots,$$

where $f^{(s)}(x) = \underbrace{f(f(\dots f(x)) \dots)}_s$.

We consider a p -adic autonomous dynamical system $\langle \mathbb{Z}_p, \mu_p, f \rangle$; for more details see, for example, [4], [5], [6], [17], [18]. The space \mathbb{Z}_p is equipped with a natural probability measure, namely, the Haar measure μ_p normalized so that $\mu_p(\mathbb{Z}_p) = 1$. Balls $B_{p^{-r}}(a)$ of nonzero radii constitute the base of the corresponding σ -algebra of measurable subsets, $\mu_p(B_{p^{-r}}(a)) = p^{-r}$. The function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is continuous on \mathbb{Z}_p .

A measurable mapping $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is called measure-preserving if

$$\mu_p(f^{-1}(U)) = \mu_p(U)$$

for each measurable subset $U \subset \mathbb{Z}_p$.

Criteria of measure-preservation for 1-Lipschitz functions are presented in the following theorems.

Theorem 1.1 (V. Anashin, [4], [5] or [9]). *A 1-Lipschitz functions $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ preserves the measure if and only if $f_k = f \pmod{p^k}$ is bijective on $\mathbb{Z}/p^k\mathbb{Z}$ for any $k = 1, 2, \dots$*

Theorem 1.2 (Theorem 2.1, [18]). *A 1-Lipschitz function $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ represented by the van der Put series 1.4 preserves the measure if and only if*

1. $\{b_0, b_1, \dots, b_{p-1}\}$ establish a complete set of residues modulo p (i.e. $f(x)$ is bijective modulo p);
2. the elements in the set $\{b_{m+p^k}, b_{m+2p^k}, \dots, b_{m+(p-1)p^k}\}$ are all nonzero residues modulo p for any $m = 0, \dots, p^k - 1$, $k \geq 2$.

Theorem 1.3 (Theorem 2.1 [17]). *A 1-Lipschitz function $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ represented in the coordinate form 1.9 preserves the measure if and only if all functions φ_0 and $\varphi_{k,[a]_k}$, $a \in \{0, 1, \dots, p^k - 1\}$, $k \geq 1$ are bijective on $\{0, \dots, p - 1\}$.*

2 Model

We consider the following automata model of encryption. Recall that $\mathfrak{A} = \langle \mathcal{T}, \mathcal{S}, \mathcal{L}, S, L \rangle$ is called an automaton if \mathcal{T} is a finite set of input symbols (input alphabet); \mathcal{L} is a finite set of output symbols (output alphabet); \mathcal{S} is a set of states (this set is not necessarily finite); $S : \mathcal{T} \times \mathcal{S} \rightarrow \mathcal{S}$ is a state transition function; $L : \mathcal{T} \times \mathcal{S} \rightarrow \mathcal{L}$ is an output function. Automaton \mathfrak{A} transforms the input words from the alphabet \mathcal{T} into the output words from the alphabet \mathcal{L} by the following rules:

1. Suppose that at some moment of discrete time k , $k \geq 0$, the automaton \mathfrak{A} is in the state $s_k \in \mathcal{S}$;
2. the symbol $t_k \in \mathcal{T}$ is fed to the input of the automaton \mathfrak{A} ;
3. as a result, the automaton \mathfrak{A} changes its state to $s_{k+1} = S(t_k, s_k)$;
4. the symbol $l_{k+1} = L(t_k, s_k) \in \mathcal{L}$ appears on the output of \mathfrak{A} .

Remember that the initial automaton $\mathfrak{A}_{s_0} = \langle \mathcal{T}, \mathcal{S}, \mathcal{L}, S, L, s_0 \rangle$ is an automaton \mathfrak{A} ; where one state $s_0 \in \mathcal{S}$ is fixed, s_0 is called the initial state.

Automaton \mathfrak{A}_{s_0} transforms the complete set of words in the alphabet \mathcal{T} into the complete set of words in the alphabet \mathcal{L} ; see Figure 1. This transformation we denote by $f_{\mathfrak{A}_{s_0}}$.

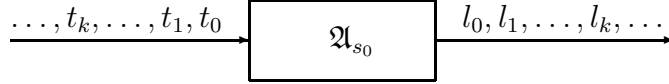


Figure 1

In particular, $f_{\mathfrak{A}_{s_0}}$ maps a set of words of length $n \in \mathbb{N}$ in the alphabet $\mathcal{T} - \mathcal{T}_n$ to the set of words of length n in the alphabet $\mathcal{L} - \mathcal{L}_n$. Such induced mapping is denoted by $f_{\mathfrak{A}_{s_0}, n}$ (i.e., $f_{\mathfrak{A}_{s_0}, n} : \mathcal{T}_n \rightarrow \mathcal{L}_n, n \in \mathbb{N}$).

As the input and output alphabets \mathcal{T} and \mathcal{L} , we consider the set $\{0, 1, \dots, p-1\} = \mathcal{T} = \mathcal{L}$, p is a prime number. The complete set of words in the alphabet $\{0, 1, \dots, p-1\}$ can be considered as \mathbb{Z}_p (i.e., the number $t_0 + pt_1 + \dots + p^k t_k + \dots$ is associated with the word $(t_0, t_1, \dots, t_k, \dots)$). In this case, $f_{\mathfrak{A}_{s_0}}$ is a map \mathbb{Z}_p to itself.

The paper [8] provides the following theorem (here we reformulate the theorem in a convenient form for further discussion).

Theorem 2.1 (V. Anashin, Theorem 2.1 [8]). *The automaton function $f_{\mathfrak{A}_{s_0}} : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ of the automaton $\mathfrak{A}_{s_0} = \langle \mathcal{T}, \mathcal{S}, \mathcal{L}, S, L, s_0 \rangle$, $\mathcal{T} = \mathcal{L} = \{0, 1, \dots, p-1\}$ is 1-Lipschitz. Conversely, for every 1-Lipschitz function $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ there exists an automaton $\mathfrak{A}_{s_0} = \langle \{0, 1, \dots, p-1\}, \mathcal{S}, \{0, 1, \dots, p-1\}, S, L, s_0 \rangle$ such that $f = \mathfrak{A}_{s_0}$.*

We assume that all induced functions $f_{\mathfrak{A}_{s_0}, n}$ are bijective on the set of words of length n , $n \geq 1$ (i.e., by the notation 1.1, $f_{\mathfrak{A}_{s_0}, n} = f_{\mathfrak{A}_{s_0}} \pmod{p^n}$ is bijective on $\mathbb{Z}/p^n\mathbb{Z}$). Then, by Theorem 1.1 1-Lipschitz function $f_{\mathfrak{A}_{s_0}}$ preserves the measure. In this case, by Proposition 4.26 from [9] the function $f_{\mathfrak{A}_{s_0}}$ is bijective on \mathbb{Z}_p .

We consider the words in the alphabet $\mathcal{T} = \{0, 1, \dots, p-1\}$ as a plain text, and the words in the alphabet $\mathcal{L} = \{0, 1, \dots, p-1\}$ as a ciphertext, then the family of bijective on \mathbb{Z}_p functions $f_{\mathfrak{A}_{s_0}}$, $s_0 \in \mathcal{S}$ defines a cipher, where the initial state s_0 is an encryption key.

Remark 2.2. Not all codes are implemented in the framework of this model of encryption. For example, the RSA cryptosystem or block ciphers can not be implemented in our encryption model. This is due to the fact that these ciphers use alphabets where the number of symbols is not a prime.

Thus, a family of bijective on \mathbb{Z}_p transformations $f_{\mathfrak{A}_{s_0}}$, $s_0 \in \mathcal{S}$, each of which implements an automaton \mathfrak{A} , form a cipher \mathfrak{C} . On \mathbb{Z}_p we set an operation "g" as the function $g : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. We say that the cipher \mathfrak{C} is a homomorphic cipher with respect to the operation "g" if for every $s_0 \in \mathcal{S}$

$$f_{\mathfrak{A}_{s_0}}(g(x, y)) = g(f_{\mathfrak{A}_{s_0}}(x), f_{\mathfrak{A}_{s_0}}(y)), \quad x, y \in \mathbb{Z}_p.$$

Suppose that operations "g₁" and "g₂" (it is possible to consider more than two operations) are defined on \mathbb{Z}_p , that is $g_1 : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $g_2 : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. We call a cipher \mathfrak{C} a fully homomorphic with respect to the operations "g₁" and "g₂", if

$$\begin{aligned} f_{\mathfrak{A}_{s_0}}(g_1(x, y)) &= g_1(f_{\mathfrak{A}_{s_0}}(x), f_{\mathfrak{A}_{s_0}}(y)), \quad x, y \in \mathbb{Z}_p; \\ f_{\mathfrak{A}_{s_0}}(g_2(x, y)) &= g_2(f_{\mathfrak{A}_{s_0}}(x), f_{\mathfrak{A}_{s_0}}(y)), \quad x, y \in \mathbb{Z}_p. \end{aligned}$$

Thus, the problem of describing homomorphic (fully homomorphic) ciphers in the p-adic model of encryption is as follows.

Find all functions $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ such that

1. f is 1-Lipschitz function (i.e., f is realized by some automaton);
2. f preserves the measure (ensures the uniqueness of decryption);
3. f defines a homomorphism with respect to a given set of operations on \mathbb{Z}_p (one operation is for a homomorphic cipher, two operations are for a fully homomorphic cipher).

3 Homomorphic ciphers

In this section we give a description of 1-Lipschitz functions $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, which preserve the measure and define the homomorphism relative to a binary operation on \mathbb{Z}_p , i.e., to some function $g : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. In this section we shall consider only the following operations:

1. ordinary arithmetical operations "+" and "·" on \mathbb{Z}_p ;
2. coordinate-wise logical operations "XOR" and "AND". These operations are defined on \mathbb{Z}_p as follows. Let p -adic numbers $x, y \in \mathbb{Z}_p$ be defined in the canonical form, i.e.,

$$x = x_0 + x_1p + \dots + x_kp^k + \dots; \quad y = y_0 + y_1p + \dots + y_kp^k + \dots,$$

where $x_i, y_i \in \{0, 1, \dots, p-1\}$, $i \geq 0$. Then the canonical representations of the p -adic numbers $x \text{ XOR } y$ and $x \text{ AND } y$ have the forms

$$x\text{XOR}y = ((x_0 + y_0) \bmod p) + ((x_1 + y_1) \bmod p)p + \dots \\ + ((x_k + y_k) \bmod p)p^k + \dots;$$

$$x\text{AND}y = ((x_0 \cdot y_0) \bmod p) + ((x_1 \cdot y_1) \bmod p)p + \dots \\ + ((x_k \cdot y_k) \bmod p)p^k + \dots;$$

Note that the functions that define the homomorphisms with respect to arithmetic operations "+" and "." on the p -adic analogue of the field of complex numbers were considered in [10]. In contrast to this case, we consider the functions that preserve the measure and define the homomorphism on \mathbb{Z}_p for a wider set of binary operations. Full description of measure-preserving, 1-Lipschitz functions, which define homomorphisms for specific operations on \mathbb{Z}_p , are presented in Theorem 3.1 (for arithmetic operations) and Theorem 3.3 (for logical operations). In other words, these theorems provide a description of all homomorphic ciphers with respect to each of the operations "+", ".", "XOR" and "AND". Note that functions that equal identically zero or one are not considered in these theorems.

Theorem 3.1 (Arithmetic operations). *Let $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be a 1-Lipschitz function, which differs from zero and unit functions.*

Then

1. *f defines a homomorphism with respect to the operation "+", i.e.,
 $f(x + y) = f(x) + f(y)$, $x, y \in \mathbb{Z}_p$ if and only if
 $f(x) = Ax$, $A \in \mathbb{Z}_p$, $A \neq 0$.*

Such a function preserves the measure if and only if $A \not\equiv 0 \pmod{p}$;

2. *f defines a homomorphism with respect to the operation ".", i.e.,
 $f(x \cdot y) = f(x) \cdot f(y)$, $x, y \in \mathbb{Z}_p$ if and only if*

$$f(x) = \begin{cases} p^k A^k (t_0^s \bmod p) \cdot (1 + p t)^a, & \text{if } x = p^k(t_0 + tp), \\ 0, & \text{if } x = 0 \end{cases} \quad (3.1)$$

where $t_0 \not\equiv 0 \pmod{p}$, $t \in \mathbb{Z}_p$, $a, A \in \mathbb{Z}_p$, $s \in \{1, \dots, p-1\}$, $k \geq 0$.

*Such a function preserves the measure if and only if
 $A \not\equiv 0 \pmod{p}$, $\text{GCD}(s, p-1) = 1$, $a \not\equiv 0 \pmod{p}$.*

Proof. Let f define a homomorphism with respect to the operation "+". Then $f(m) = m \cdot f(1)$, $m \in \mathbb{Z}$. Let $f(1) = A \in \mathbb{Z}_p$, $A \neq 0$. Since 1-Lipschitz function f is continuous on \mathbb{Z}_p and \mathbb{Z} is dense in \mathbb{Z}_p , then $f(x) = A \cdot x$, $x \in \mathbb{Z}_p$. The function $f(x) = A \cdot x$ preserves the measure if and only if $A \not\equiv 0 \pmod{p}$ (see, for example, Lemma 4.41 in [9]). It is clear that the function $f(x) = Ax$ defines a homomorphism with respect to addition on \mathbb{Z}_p .

Let us prove the second statement of the theorem. Let f defines a homomorphism with respect to multiplication on \mathbb{Z}_p . Since f is distinct from the identity and zero functions (i.e., there are $x, y \in \mathbb{Z}_p$ such that $f(x) \neq 1$ and $f(y) \neq 0$), and f is the homomorphism, then $f(0) = 0$. Moreover, since f is the homomorphism, then $f(1) = 1$. As f is a 1-Lipschitz function, then $f(p) \equiv 0 \pmod{p}$ and $f(1+pt) \equiv 1 \pmod{p}$. 1-Lipschitz function f induces a mapping $f_0 : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, $z \mapsto f(z) \pmod{p^k}$. Because f is the homomorphism, then f_0 is also homomorphic on $\mathbb{Z}/p\mathbb{Z}$ with respect to multiplication. The function f_0 is a non-zero function (otherwise, $f(1+pt) \equiv f_0(1) \equiv 0 \pmod{p}$). Then there exists $s \in \{0, 1, \dots, p-2\}$ such that $f_0(z) = z^s$. Let $f(p) = pA$, $A \in \mathbb{Z}_p$.

Since any $x \in \mathbb{Z}_p$, $x \neq 0$ can be represented in the form

$$x = p^r t_0(1 + pt), \quad t \in \mathbb{Z}_p, \quad t_0 \in \{1, 2, \dots, p-1\}, \quad r \geq 0,$$

then the function f , which defines a homomorphism with respect to multiplication on \mathbb{Z}_p , can be represented in the form

$$f(x) = \begin{cases} p^k \cdot A^k \cdot (t_0^s \pmod{p}) \cdot \phi(1 + pt), & \text{if } x = p^k(t_0 + t \cdot p), \quad k \geq 0, \\ 0, & \text{if } x = 0 \end{cases}$$

where $t_0 \not\equiv 0 \pmod{p}$, $t \in \mathbb{Z}_p$, $a, A \in \mathbb{Z}_p$, $s \in \{0, 1, \dots, p-2\}$ (here we consider the function $t_0^s \pmod{p}$ as a mapping of the set $\{1, 2, \dots, p-1\}$ into itself), and 1-Lipschitz function $\phi : 1+p\mathbb{Z}_p \rightarrow 1+p\mathbb{Z}_p$ define a homomorphism with respect to multiplication on $1+p\mathbb{Z}_p$.

Let us find the representation of the function ϕ . Let $\text{EXP}_p : p\mathbb{Z}_p \rightarrow 1+p\mathbb{Z}_p$ be the p -adic exponent and $\text{LN}_p : 1+p\mathbb{Z}_p \rightarrow p\mathbb{Z}_p$ be the p -adic logarithm. We consider the function $g : p\mathbb{Z}_p \rightarrow p\mathbb{Z}_p$ such that $g(\tau) = \text{LN}_p(\phi(\text{EXP}_p(\tau)))$. Then, the function g defines a homomorphism with respect to addition on $p\mathbb{Z}_p$:

$$\begin{aligned} g(\tau_1 + \tau_2) &= \text{LN}_p(\phi(\text{EXP}_p(\tau_1 + \tau_2))) = \\ &= \text{LN}_p(\phi(\text{EXP}_p(\tau_1) \cdot \text{EXP}_p(\tau_2))) = \\ &= \text{LN}_p(\phi(\text{EXP}_p(\tau_1)) \cdot \phi(\text{EXP}_p(\tau_2))) = \\ &= \text{LN}_p(\phi(\text{EXP}_p(\tau_1))) + \text{LN}_p(\phi(\text{EXP}_p(\tau_2))) = \\ &= g(\tau_1) + g(\tau_2). \end{aligned}$$

Therefore, there exists $a \in \mathbb{Z}_p$ such that $g(\tau) = a\tau$. Since $\text{EXP}_p(\text{LN}_p(1 + pz)) = 1 + pz$, $z \in \mathbb{Z}_p$, then

$$\text{EXP}_p(g(\tau)) = \text{EXP}_p(a \cdot \tau) = \text{EXP}_p(\tau)^a = \phi(\text{EXP}_p(\tau)).$$

Let $x = 1 + pt = \text{EXP}_p(\tau)$, $\tau \in p\mathbb{Z}_p$. Then $\phi(x) = x^a$, $a \in \mathbb{Z}_p$.

Thus, the function f can be represented in the form

$$f(x) = f(p^k t_0(1 + pt)) = p^k \cdot A^k \cdot (t_0^s(\text{mod } p)) \cdot (1 + pt)^a.$$

Performing the corresponding calculations, we see that the function of this type defines a homomorphism on \mathbb{Z}_p with respect to multiplication.

Let us find the values $A, a \in \mathbb{Z}_p$, $s \in \{1, 2, \dots, p-1\}$, where the function f of the form 3.1 preserves the measure. For this we use the criterion of Theorem 1.2. Let us find the value of the van der Put coefficients of the function f . Let $t \in \{0, 1, \dots, p^r-1\}$, $t_0 \in \{1, \dots, p-1\}$, $h \in \{1, 2, \dots, p-1\}$, $k \geq 0$. Then $B_0 = f(0) = 0$ and

$$\begin{aligned} b_{t_0 p^k + t p^{k+1} + p^{k+r} h} &= \frac{1}{p^{k+r}} B_{t_0 p^k + t p^{k+1} + p^{k+r} h} \equiv \\ &\equiv \frac{1}{p^{k+r}} (f(t_0 p^k + t p^{k+1} + p^{k+r} h) - f(t_0 p^k + t p^{k+1})) \equiv \\ &\equiv a \cdot A^k \cdot (t_0^s(\text{mod } p)) \cdot h \pmod{p}, \quad r \geq 1, \end{aligned}$$

$$b_{t_0 p^k} = \frac{1}{p^k} B_{t_0 p^k} \equiv \frac{1}{p^k} f(t_0 p^k) \equiv A^k \cdot (t_0^s(\text{mod } p)) \pmod{p}, \quad r \geq 0.$$

Since $t_0^s \not\equiv 0(\text{mod } p)$, then $\{b_{t_0 p^k + t p^{k+1} + p^{k+r} h} : h = 1, 2, \dots, p-1\}$ coincides with the set of all non-zero residues modulo p if and only if $a \not\equiv 0 \pmod{p}$, and $A \not\equiv 0 \pmod{p}$. The set $\{b_{t_0 p^k} : t_0 = 1, 2, \dots, p-1\}$ coincides with the set of all non-zero residues modulo p as $\text{GCD}(s, p-1) = 1$. Since $f(t_0 + pt) \equiv t_0^s \pmod{p}$, $t_0 \in \{1, \dots, p-1\}$ and $f(0) = 0$, then $f(\text{mod } p)$ is bijective on $\mathbb{Z}/p\mathbb{Z}$. Then, by Theorem 1.2 the function f preserves the measure if and only if

$$a \not\equiv 0 \pmod{p}; \quad A \not\equiv 0 \pmod{p}; \quad \text{GCD}(s, p-1) = 1.$$

□

Remark 3.2. If in 3.1 we set $a = n$, $s = n$, $A = p^{n-1}$ for some $n \in \mathbb{N}$, then $f(x) = x^n$. That is, all such polynomials define a homomorphism with respect to multiplication on \mathbb{Z}_p . Functions of the form $f(x) = x^n$ for $n \geq 1$ do not preserve the measure.

Theorem 3.3 (Logical operations). *Let $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be a 1-Lipschitz function defined in the coordinate form, i.e.,*

$$f(x) = f(x_0 + \dots + p^k x_k + \dots) = \sum_{k=0}^{\infty} p^k \varphi_k(x_0, \dots, x_k),$$

where $\varphi_k(x_0, \dots, x_k)$ are p -valued logical functions. Then

1. f defines a homomorphism with respect to the operation "XOR" if and only if

$$\varphi_k(x_0, \dots, x_k) = \alpha_0^{(k)} x_0 + \alpha_1^{(k)} x_1 + \dots + \alpha_k^{(k)} x_k,$$

where $\alpha_i^{(k)} \in \{0, \dots, p-1\}$, $0 \leq i \leq k$, $k \geq 0$.

Such functions preserve the measure if and only if $\alpha_k^{(k)} \not\equiv 0 \pmod{p}$, $k \geq 0$;

2. f defines a homomorphism with respect to the operation "AND" if and only if

$$\varphi_k(x_0, \dots, x_k) = x_0^{s_0^{(k)}} \cdot x_1^{s_1^{(k)}} \cdots x_k^{s_k^{(k)}},$$

where $s_i^{(k)} \in \{1, \dots, p-1\}$, $0 \leq i \leq k$, $k \geq 0$.

Such functions preserve the measure if and only if

$$f(x) = f(x_0 + px_1 + \dots + p^k x_k + \dots) = \sum_{k=0}^{\infty} p^k (x_k^{s_k^{(k)}} \pmod{p}),$$

where $\text{GCD}(s_k^{(k)}, p-1) = 1$, $k \geq 0$.

Proof. Let f define a homomorphism with respect to the operation "XOR" on \mathbb{Z}_p , i.e., $\varphi_k(x_0 + y_0, \dots, x_k + y_k) = \varphi_k(x_0, \dots, x_k) + \varphi_k(y_0, \dots, y_k)$, $x_i, y_j \in \{0, 1, \dots, p-1\}$, $k \geq 0$.

Let

$$\varphi_{k,r}(x) = \varphi_k(\underbrace{0, \dots, 0}_r, x, 0, \dots, 0), \quad 0 \leq r \leq k.$$

Since $\varphi_{k,r}(x + y) = \varphi_{k,r}(x) + \varphi_{k,r}(y)$, $x, y \in \mathbb{Z}/p\mathbb{Z}$, then $\varphi_{k,r}(x)$ is the homomorphism on $\mathbb{Z}/p\mathbb{Z}$ with respect to addition. Therefore, $\varphi_{k,r}(x) = a_r^{(k)} x$, $a_r \in \mathbb{Z}/p\mathbb{Z}$. Since

$$\varphi_k(x_0, \dots, x_k) = \varphi_{k,0}(x_0) + \dots + \varphi_{k,k}(x_k),$$

then $\varphi_k(x_0, \dots, x_k) = a_0^{(k)} x_0 + a_1^{(k)} x_1 + \dots + a_k^{(k)} x_k$, $k \geq 0$, where $a_i^{(j)} \in \{0, \dots, p-1\}$.

It is clear that a function represented by the coordinate functions defines a homomorphism on \mathbb{Z}_p with respect to the operation "XOR".

Let

$$f(x) = f(x_0 + x_1p + \dots) = \sum_{k=0}^{\infty} ([a_0^{(k)}x_0 + a_1^{(k)}x_1 + \dots + a_k^{(k)}x_k](\text{mod } p))p^k.$$

Here, by the notation $(*)(\text{mod } p)$, we emphasize the fact that φ_k is defined by the operations on $\mathbb{Z}/p\mathbb{Z}$. Coordinate sub-functions of the function f from the representation 1.9 have the form $c + a_k^{(k)}x_k$, $c \in \{0, \dots, p-1\}$. These sub-functions are bijective on $\mathbb{Z}/p\mathbb{Z}$ as $a_k^{(k)} \not\equiv 0 \pmod{p}$. Thus, by Theorem 1.3 the function f preserves the measure as soon as $a_k^{(k)} \not\equiv 0 \pmod{p}$, $k \geq 0$.

Let us prove the second statement of the theorem. Let f be a homomorphism with respect to the operation "AND" on \mathbb{Z}_p , i.e.,

$$\begin{aligned} \varphi_k(x_0 \cdot y_0, \dots, x_k \cdot y_k) &= \\ &= \varphi_k(x_0, \dots, x_k) \cdot \varphi_k(y_0, \dots, y_k), \quad x_i, y_j \in \{0, 1, \dots, p-1\}, \quad k \geq 0. \end{aligned}$$

Let

$$\varphi_{k,r}(x) = \varphi_k(\underbrace{1, \dots, 1}_r, x, 1, \dots, 1), \quad 0 \leq r \leq k.$$

Since $\varphi_{k,r}(x \cdot y) = \varphi_{k,r}(x) \cdot \varphi_{k,r}(y)$, $x, y \in \mathbb{Z}/p\mathbb{Z}$, then $\varphi_{k,r}(x)$ is the homomorphism on $\mathbb{Z}/p\mathbb{Z}$ with respect to multiplication. Therefore, $\varphi_{k,r}(x) = x^{s_r^{(k)}}$, $s_r \in \{0, 1, \dots, p-2\}$. Since

$$\varphi_k(x_0, \dots, x_k) = \varphi_{k,0}(x_0) \cdots \varphi_{k,k}(x_k),$$

then $\varphi_k(x_0, \dots, x_k) = x_0^{s_0^{(k)}} \cdot x_1^{s_1^{(k)}} \cdots x_k^{s_k^{(k)}}$, $k \geq 0$ (φ_k is given through the operations on $\mathbb{Z}/p\mathbb{Z}$).

It is clear that a function represented by the coordinate functions defines a homomorphism on \mathbb{Z}_p with respect to the operation "AND".

Let

$$f(x) = f(x_0 + x_1p + \dots) = \sum_{k=0}^{\infty} ([x_0^{s_0^{(k)}} \cdot x_1^{s_1^{(k)}} \cdots x_k^{s_k^{(k)}}](\text{mod } p))p^k.$$

Here φ_k is also defined by the operations on $\mathbb{Z}/p\mathbb{Z}$.

Coordinate sub-functions of the function f from the representation 1.9 have the form $a_0^{s_0^{(k)}} \cdot a_1^{s_1^{(k)}} \cdots a_{k-1}^{s_{k-1}^{(k)}} \cdot x_k^{s_k^{(k)}}$, $a_i^{s_i} \in \{0, \dots, p-1\}$, $0 \leq i \leq k-1$. These sub-functions are bijective on $\mathbb{Z}/p\mathbb{Z}$ as soon as $a_0^{s_0^{(k)}} \cdot a_1^{s_1^{(k)}} \cdots a_{k-1}^{s_{k-1}^{(k)}} \equiv 1$

$(\text{mod } p)$ for any $a_i \in \{0, \dots, p-1\}$, $0 \leq i \leq k-1$ (this is equivalent to $s_0^{(k)} \equiv s_1^{(k)} \equiv \dots \equiv s_{k-1}^{(k)} \equiv 0 \pmod{p}$) and $\text{GCD}(s_k^{(k)}, p-1) = 1$.

Thus, by Theorem 1.3 the function f preserves the measure as soon as $s_0^{(k)} \equiv s_1^{(k)} \equiv \dots \equiv s_{k-1}^{(k)} \equiv 0 \pmod{p}$ and $\text{GCD}(s_k^{(k)}, p-1) = 1$, $k \geq 0$. \square

4 Fully homomorphic ciphers

In this section we describe fully homomorphic ciphers with respect to each pair of operations from the set $\{“+”, “\cdot”, “\text{XOR}”, “\text{AND}”\}$. As we show in Proposition 4.1, there are no such fully homomorphic ciphers.

Therefore, we consider the following problem. Suppose there exists a homomorphic cipher with respect to the operation $“*”$. We consider $“+”$ on \mathbb{Z}_p as such an operation (these ciphers were described in Theorem 3.1). We want to find a new operation $“G”$ such that this cipher defines a homomorphism with respect to new operation $“G”$. All possible new operations for a homomorphic cipher with respect to $“+”$ are described in Proposition 4.2. As a method of setting a new operation, we consider convergent in the p -adic metric power series in two variables.

Let $\mathcal{H}(\ast)$ be the set of all non-zero and non-trivial 1-Lipschitz functions, which define a homomorphism with respect to the operation $“*”$ on \mathbb{Z}_p and preserve the measure. For arithmetic and logical coordinate-wise operations, the sets

$$\mathcal{H}(+), \mathcal{H}(\cdot), \mathcal{H}(\text{XOR}), \mathcal{H}(\text{AND}) \quad (4.1)$$

are described in Theorems 3.1 and 3.3.

The set of functions, consisting of identical function $f(x) = x$, is denoted by I .

Proposition 4.1. *In the notation 4.1 the following relations hold:*

1. $\mathcal{H}(+) \cap \mathcal{H}(\cdot) = I$;
2. $\mathcal{H}(+) \cap \mathcal{H}(\text{XOR}) = I$;
3. $\mathcal{H}(+) \cap \mathcal{H}(\text{AND}) = I$;
4. $\mathcal{H}(\cdot) \cap \mathcal{H}(\text{XOR}) = I$;
5. $\mathcal{H}(\cdot) \cap \mathcal{H}(\text{AND}) = I$;
6. $\mathcal{H}(\text{XOR}) \cap \mathcal{H}(\text{AND}) = I$;

Proof. Let us prove the first statement of the theorem. Let $f(x) \in \mathcal{H}(+) \cap \mathcal{H}(\cdot)$. As $f(x) \in \mathcal{H}(\cdot)$, then $f(1) = 1$. Thus, $f(1) = A = 1$, that is, $f(x) = x$.

Let us prove the second statement. Let $f(x) \in \mathcal{H}(+) \cap \mathcal{H}(\text{XOR})$. As $f \in \mathcal{H}(+)$, then $f(x) = Ax$, $A \in \mathbb{Z}_p$. From $f(x \text{ XOR } y) = f(x) \text{ XOR } f(y)$ it follows that $A(x \text{ XOR } y) = Ax \text{ XOR } Ay$. Suppose $x = 1$ and $y = p - 1$. Then

$$A \text{ XOR } (p - 1)A = 0. \quad (4.2)$$

It is clear that this equation holds for $A = 1$. Let $A = A_0 + A_1p + \dots$, $A_k \in \{0, \dots, p - 1\}$. Note that

$$\begin{aligned} (p - 1)A &= (p - 1)(A_0 + A_1p + \dots) = \\ &= [p - A_0] + p[A_0 - 1 + p - A_1] + p^2[A_1 - 1 + p - A_2] + \dots \end{aligned}$$

We find the values A_0, A_1, \dots , using the equality 4.2. We obtain that $p - A_0 + A_0 \equiv 0 \pmod{p}$; $A_0 - 1 + p - A_1 + A_1 \equiv 0 \pmod{p}$, i.e., $A_0 = 1$; $A_1 - 1 + p - A_2 + A_2 \equiv 0 \pmod{p}$, so $A_1 = 1$ and so on. As a result, we find that 4.2 also holds for $A = 1 + p + p^2 + \dots = \frac{1}{1-p}$. In this case

$$f(x) = Ax = A(x_0 + px_1 + \dots) = \sum_{k=0}^{\infty} (x_0 + x_1 + \dots + x_k)p^k. \quad (4.3)$$

We represent this function in the coordinate form 1.7. Here, we denote the operation of addition on $\mathbb{Z}/p\mathbb{Z}$ by " \oplus ". Note that relation 4.3 for the function f implies that $\varphi_0 = x_0$, $\varphi_1(x_0, x_1) = x_0 \oplus x_1$, $x_0 + x_1 = x_0 \oplus x_1 + p\delta(x_0, x_1)$, where $\delta(x_0, x_1) = \frac{x_0 + x_1 - x_0 \oplus x_1}{p}$. Since $f \in \mathcal{H}(\text{XOR})$, then $c_0, c_1, c_2 \in \{0, \dots, p - 1\}$ should exist such that $\varphi_2 = c_0x_0 \oplus c_1x_1 \oplus c_2x_2 = x_0 \oplus x_1 \oplus x_2 + \delta(x_0, x_1)$. Since $\delta(0, 0) = 0$, then $c_2 = 1$. Suppose $x_2 = 0$, $x_1 = 0$ and $x_0 = 0$, then $c_0 = 1$, $c_1 = 1$. Then $\frac{x_0 + x_1 - x_0 \oplus x_1}{p} = 0$ for $x_2 = 0$ and $x_0 + x_1 = x_0 \oplus x_1$.

This contradiction shows that this type of coordinate representation of the function f from 4.3 does not coincide with the representation of the second statement of the Theorem 3.3 (or $f \notin \mathcal{H}(\text{XOR})$). Then $f(x) = x$ and $\mathcal{H}(+) \cap \mathcal{H}(\text{XOR}) = I$.

Let us prove statement 3. Suppose that $f(x) \in \mathcal{H}(+) \cap \mathcal{H}(\text{AND})$, then we obtain $f(p^k) = p^k = Ap^k$. Then $A = 1$ and $\mathcal{H}(+) \cap \mathcal{H}(\text{AND}) = I$.

Let us prove statement 4. Let $f \in \mathcal{H}(\cdot) \cap \mathcal{H}(\text{XOR})$. As $1 + p + p^2t = 1 \text{ XOR } (p + p^2t)$, then

$$\begin{aligned} 1 + pA(1 + pt)^a &= 1 \text{ XOR } pA(1 + pt) = \\ &= 1 \text{ XOR } f(p(1 + pt)) = f(1 \text{ XOR } (p + p^2t)) = \\ &= f(1 + p + p^2t) = (1 + p + p^2t)^a \end{aligned} \quad (4.4)$$

Set $t = 0$ in 4.4 and differentiate functions from 4.4, then we get

$$1 + pA = (1 + p)^a \quad \text{and} \quad A = \left(\frac{1}{1 + pt} + p \right)^{a-1}. \quad (4.5)$$

Set $t = 0$ in 4.5, we get $A = (1 + p)^{a-1}$ and $1 + pA = (1 + p)A$. Thus $a = A = 1$.

Using the representation of the second statement of the Theorem 3.1 and the second statement of 3.3 for the function f for $t \in t_0 + p\mathbb{Z}_p$, $t_0 \neq 0$, we get

$$\alpha_0^{(0)} t_0 \equiv f(t) \equiv t_0^s \pmod{p}.$$

Then $\alpha_0^{(0)} = 1$, $s = 1$ and the function f can be represented in the form

$$f(x) = \begin{cases} p^k t, & \text{if } x = p^k t, t \not\equiv 0 \pmod{p}, k > 0; \\ t, & \text{if } x = t, t \not\equiv 0 \pmod{p}, k = 0; \\ 0, & \text{if } x = 0. \end{cases}$$

Thus, $f(x) = x$ and $\in \mathcal{H}(+) \cap \mathcal{H}(\text{AND}) = I$.

Let us prove statement 5. Let $f \in \mathcal{H}(\cdot) \cap \mathcal{H}(\text{AND})$. Let $x = x_0 + px_1 + \dots + x_k p^k + \dots$, $x_i \in \{0, \dots, p-1\}$. Taking into account the type of representation of functions from $\mathcal{H}(\cdot)$ and $\mathcal{H}(\text{AND})$, we obtain that

$$p^k x_k^{s_k} = f(x_k p^k) = p^k A^k (x_k^s \pmod{p}).$$

Then, $s_k = s$, $k \geq 0$, $A = 1$. Taking into account the representation of f from Theorem 3.1 and Theorem 3.3, we get

$$\begin{aligned} (1 + pt)^a &= f(1 + pt) = f(1 + pt_1 + \dots) = \\ &= 1 + p(t_1^s \pmod{p}) + \dots + p^k(t_k^s \pmod{p}) + \dots \end{aligned}$$

Let us find the values of the van der Put coefficients for each representation of the function f . Let $1 + pt + p^k h = 1 + pt_1 + \dots + p^{k-1} t_{k-1} + p^k h$, $h \not\equiv 0 \pmod{p}$, then

$$\begin{aligned} B_{1+pt+p^k h} &= (1 + pt + p^k h)^a - (1 + pt)^a = ah(1 + pt)^{a-1} p^k = \\ &= (1 + \dots + p^{k-1}(t_{k-1}^s \pmod{p}) + p^k(h^s \pmod{p})) - \\ &\quad - (1 + \dots + p^{k-1}(t_{k-1}^s \pmod{p})) = h^s \pmod{p} p^k. \end{aligned}$$

As $ah(1 + pt)^{a-1} p^k = h^s \pmod{p}$, then $a = 1$, $s = 1$. Thus,

$$f(x) = \begin{cases} p^k t, & \text{if } x = p^k t, t \not\equiv 0 \pmod{p}, k > 0; \\ t, & \text{if } x = t, t \not\equiv 0 \pmod{p}, k = 0; \\ 0, & \text{if } x = 0, \end{cases}$$

That is $f(x) = x$ and $\mathcal{H}(\cdot) \cap \mathcal{H}(\text{AND}) = I$.

Let us prove statement 6. Let $f \in \mathcal{H}(\text{XOR}) \cap \mathcal{H}(\text{AND})$. Using the coordinate representation of the function f (Theorem 3.3), we obtain

$$\alpha_0^{(k)} x_0 + \alpha_1^{(k)} x_1 + \dots + \alpha_k^{(k)} x_k = x_k^{s_k^{(k)}}, \quad k \geq 0.$$

Then, $\alpha_0^{(k)} x_0 + \alpha_1^{(k)} x_1 + \dots + \alpha_{k-1}^{(k)} x_{k-1}$ is a constant as soon as

$$\alpha_0^{(k)} = \dots = \alpha_{k-1}^{(k)} = 0, \quad \alpha_k^{(k)} = 1, \quad s_k^{(k)} = 1.$$

Thus, $f(x) = x$ and $\mathcal{H}(\text{XOR}) \cap \mathcal{H}(\text{AND}) = I$. □

Proposition 4.1 shows that there are no fully homomorphic ciphers for all pairs of arithmetic and coordinate-wise logical operations. However, we may reformulate the problem of finding fully homomorphic ciphers as follows. Let $*$ be an operation on \mathbb{Z}_p , and $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be a family of 1-Lipschitz functions that preserve the measure. Then we define a homomorphism with respect to this operation. We find operation G on \mathbb{Z}_p such that each function f defines a homomorphism with respect to this operation, and that G differs from $*$, i.e., $f(G(x, y)) = G(f(x), f(y))$, $x, y \in \mathbb{Z}_p$. As a result, we find that the function f defines a homomorphism with respect to both operations $*$ and G , i.e., the family of functions f can be used as a fully homomorphic cipher. As new operation G , we consider an arbitrary mapping $G : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. Of course, such an operation may not be associative, commutative, etc.

In Proposition 4.2 we give a description of all operations G (defined by power series), where linear functions $f(x) = Ax$, $A \in \mathbb{Z}_p$ define the homomorphism with respect to the operation G . In other words, f is the homomorphism with respect to addition and to new operation G .

We set G (a function $G : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$) as the convergent power series in $\mathbb{Z}_p \times \mathbb{Z}_p$ (it is sufficient to require that the general term of the series converges to zero in the p -adic metric).

The function $G(x, y)$ is given by the convergent power series

$$G(x, y) = c + ax + by + \sum_{k=1}^{\infty} \sum_{i+j=n_k} c_{i,j} x^i y^j, \quad c_{i,j}, a, b, c \in \mathbb{Z}_p, \quad (4.6)$$

where for any $n_k \in \{n_1, n_2, \dots \mid n_k \in \mathbb{N}, 1 < n_1 < n_2 < \dots\} = \mathcal{N}_G$ there exists $0 \leq i, j \leq n_k$ such that $c_{i,j} \neq 0$, and if $n \notin \mathcal{N}_G$, then $c_{i,j} = 0$ for any $0 \leq i, j \leq n_k$, $i + j = n$.

Proposition 4.2. *Let $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $f(x) = Ax$, $A \in \mathbb{Z}_p$, $A \neq 0$. The function f defines a homomorphism with respect to the operation " G ", given as the series 4.6 if and only if for $\mathcal{N}_G \neq \emptyset$:*

1. $c = 0$;
2. $n_k = dq_k + 1$, $k \geq 1$, where $d = \text{GCD}(n_1 - 1, n_2 - 1, \dots, n_k - 1, \dots)$, $q_k \in \mathbb{N}$;
3. $A^d = 1$

and $G = ax + by$ for any $A \neq 0$ for $\mathcal{N}_G = \emptyset$.

Proof. Let $f = Ax$ define a homomorphism with respect to the operation " G ", i.e., $AG(x, y) = G(Ax, Ay)$ and $\mathcal{N}_G \neq \emptyset$. Using the representation 4.6, we get that A satisfies the system of equations

$$A^{n_1} = A, A^{n_2} = A, \dots, A^{n_k} = A, \dots$$

or $A^{n_k-1} = 1$, $k \geq 1$. This system of equations is equivalent to the equation $A^d = 1$, where $d = \text{GCD}(n_1 - 1, n_2 - 1, \dots, n_k - 1, \dots)$. Let $x = 0$, $y = 0$, then $Ac = c$ and $c = 0$ (since $A \neq 0$). It is easy to see that under the conditions of the proposition, the function $f(x) = Ax$ defines homomorphism with respect to the operation " G ". If $\mathcal{N}_G = \emptyset$, then $G(x, y) = c + ax + ay$ and $c = 0$. The function $f(x) = Ax$ defines the homomorphism with respect to $G = ax + by$ for any A . \square

Remark 4.3. Here we recall known facts about the number of solutions of the equation $A^d = 1$ in \mathbb{Z}_p . If $p \nmid d$, then the equation $A^d = 1$ has $\text{GCD}(d, p - 1)$ solutions in \mathbb{Z}_p (see, for example, Theorem 3.24 in [9]). If $d = p^k$, then the equation $A^{p^k} = 1$ has a unique solution $A = 1$, except when $p = 2$ and $k = 1$ (in this case, the equation $A^2 = 1$ in \mathbb{Z}_2 has solutions $A = 1$, $A = -1$; see, for example, Theorem 18.9 in [15]). Clearly, for $d = p^k n$, $p \nmid d$ the equation $A^d = 1$ has $\text{GCD}(n, p - 1)$ solutions in \mathbb{Z}_p .

Thus, for $\mathcal{N}_G \neq \emptyset$, maximum number of functions of the form $f(x) = Ax$, which define the homomorphism with respect to the operation " G ", equals $p - 1$. If the functions $f(x) = Ax$ are chosen for the construction of fully homomorphic ciphers with respect to operations "+" and " G ", the prime number p must be large.

Example 4.4. Here are some examples of operations " G ", for which the functions $f(x) = Ax$ define the homomorphism with respect to the operations "+" and " G " for a suitable choice of A :

1. $G(x, y) = ax + by$, $a, b \in \mathbb{Z}_p$ for any $A \in \mathbb{Z}_p$, $A \neq 0$;
2. $G_1(x, y) = xy^{p-1}$ or $G_2(x, y) = x^{p-1}y + xy^{p-1}$ for $A \in \mathbb{Z}_p$, $A^{p-1} = 1$.
The operation G_2 is commutative;
3. for $p \neq 2$, then $G(x, y) = x^{\frac{p-1}{2}} \cdot y^{\frac{p-1}{2}}$, $A^{p-1} = 1$;
4. $G(x, y) = \sum_{s=0}^{\infty} p^s (x^{(p-1)s+1} + y^{(p-1)s+1}) = \frac{x}{1-px^{p-1}} + \frac{y}{1-py^{p-1}}$, and $A^{p-1} = 1$.

5 Application

In Proposition 4.1 we have shown that a fully homomorphic cipher does not exist (within the p -adic model of encryption) for each pair of operations from the set $\{“+”, “\cdot”, “XOR”, “AND”\}$. Suppose that, using the pairs of operations from this set, we can write an equation that can be implemented by a computer program. From this perspective, the result of Proposition 4.1 means that within the p -adic model of encryption there are no "universal" (i.e., for any software) fully homomorphic ciphers. However, as was shown in Proposition 4.2, it is possible to construct a fully homomorphic cipher with respect to a pair of "new" operations on \mathbb{Z}_p . In this section we will discuss such a possibility.

We assume that in the framework of the p -adic model of encryption a computer program implements a formula of the original data. This formula is written using the set of operations $g_1 : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ and $g_2 : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. By analogy with the formulas of Boolean algebra, let us define formulas with respect to the operations g_1 and g_2 over \mathbb{Z}_p :

1. variables and operations g_1, g_2 are formulas;
2. if F_1, F_2 are formulas, then $g_1(F_1, F_2), g_2(F_1, F_2)$ are formulas.

We denote the set of all formulas defined with respect to operations g_1 and g_2 as $[g_1, g_2]$. For instance, $x^3 + y + y^2 \cdot z$ is the formula from the set $[“+”, “\cdot”]$. The following assertion holds.

Proposition 5.1. *Let operations $g_1 : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ and $g_2 : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ be defined by the formulas from $[“+”, “\cdot”]$. Let 1-Lipschitz function $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ define a nontrivial homomorphism with respect to the operations g_1 and g_2 .*

Then $[g_1, g_2] \subset [“+”, “\cdot”]$ and $[g_1, g_2] \neq [“+”, “\cdot”]$.

Proof. Since $g_1, g_2 \in [“+”, “.”]$, then $[g_1, g_2] \subset [“+”, “.”]$. Assume that $[g_1, g_2] = [“+”, “.”]$. Then “+” and “.” are defined by the formulas $\Psi_{“+”}(x_1, x_2)$ and $\Psi_{“.”}(x_1, x_2)$ with respect to the operations g_1 and g_2 . Since f is a homomorphism with respect to g_1 and g_2 , then

$$\begin{aligned} f(x_1 + x_2) &= f(\Psi_{“+”}(x_1, x_2)) = \Psi_{“+”}(f(x_1), f(x_2)) = f(x_1) + f(x_2); \\ f(x_1 \cdot x_2) &= f(\Psi_{“.”}(x_1, x_2)) = \Psi_{“.”}(f(x_1), f(x_2)) = f(x_1) \cdot f(x_2); \end{aligned}$$

i.e. f is the homomorphism with respect to “+” and “.”. Then from Proposition 4.1 it follows that f is an identity mapping. This contradicts the condition of the Proposition. \square

Proposition 5.1 shows that if a fully homomorphic cipher exists with respect to certain operations g_1 and g_2 (formulas with respect to arithmetic operations “+” and “.”), then the cipher is not applicable for all formulas from $[“+”, “.”]$. Previously, we assumed the class $[“+”, “.”]$ was “universal” in the sense that any computer program could implement the formula from this class.

In this regard, we propose the following method using a fully homomorphic encryption to secure remote computing within the p -adic model of encryption.

Let $W(d_1, \dots, d_n)$ be a given formula (or program), by which cloud computing will be performed. Here $d_1, \dots, d_n \in \mathbb{Z}_p$ stand for data. This formula can be given, for example, in the basis of the usual arithmetic operations. Let us find a new pair of operations g_1 and g_2 , such that:

1. the formula $W \in [g_1, g_1]$;
2. fully homomorphic cipher f_a with respect to the operations g_1 and g_2 exists, where a is the key and $[g_1, g_1] \neq [“+”, “.”]$.

Then $W(f_a(d_1), \dots, f_a(d_n)) = f_a(W(d_1, \dots, d_n))$. As a result, we are able to perform cloud computing in secure mode for a given formula (program) W .

Example 5.2. Let

$$W(x, y, z) = x^{p-1}y^{(p-1)^2}z + x^{p-1}y^{p-1}z + x^py^{p(p-1)}(1 + y^{p^2-3p+2})$$

be a formula by which cloud computing will be performed.

Let us consider the operation of usual addition “+” in \mathbb{Z}_p , and the operation “*” in \mathbb{Z}_p defined by $a * b = ab^{p-1}$. Then

$$W(x, y, z) = z * (x * y) + (z * x) * y + (x * x) * (y * y) + x * ((x * y) * y).$$

From Proposition 4.1 it follows that the functions $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $f(x) = Ax$, $A \in \mathbb{Z}_p$, $A \neq 0$ and $A^{p-1} = 1$ define the homomorphisms with respect to operations "+" and "*". In other words, the family of such functions is a fully homomorphic cipher with respect to the given operations. In particular, $f(W(x, y, z)) = W(f(x), f(y), f(z))$.

References

- [1] Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. (2015). CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. *Expert Systems with Applications*, 42(21), 7905–7916.
- [2] https://en.wikipedia.org/wiki/Homomorphic_encryption. Cited 2015-07-14
- [3] Daniele Micciancio (2010-03-01). "A First Glimpse of Cryptography's Holy Grail". Association for Computing Machinery. p. 96. Retrieved 2010-03-17.
- [4] V. Anashin, Uniformly distributed sequences of p -adic integers, *Mathematical Notes*. 55(1994) 109–133.
- [5] V. Anashin, Uniformly distributed sequences of p -adic integers, II, *Discrete Math. Appl.* 12(6)(2002) 527–590.
- [6] Anashin V 2006 Ergodic Transformations in the Space of p -adic Integers *Proc. Int. Conf. on p -adic Mathematical Physics* (Belgrade, Serbia and Montenegro) vol 826 (AIP Conference Proceedings) pp 3–24
- [7] V. Anashin, Automata finiteness criterion in terms of van der Put series of automata functions P -Adic Numbers, *Ultrametric Analysis, and Applications*, February 2012, Volume 4, Issue 2, pp 151-160
- [8] V. Anashin, The Non-Archimedean Theory of Discrete Systems, *Mathematics in Computer Science* December 2012, Volume 6, Issue 4, pp 375-393
- [9] V. Anashin, A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics vol 49, Walter de Gruyter (Berlin — New York), 2009.
- [10] W.H. Schikhof, *Ultrametric calculus. An introduction to p -adic analysis*, Cambridge: Cambridge University Press, 1984.

- [11] Fully Homomorphic Encryption over the Integers Marten van Dijk MIT, Craig Gentry IBM Research, Shai Halevi IBM Research, Vinod Vaikuntanathan IBM Research, June 8, 2010
- [12] M. Van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan. Fully homomorphic encryption over the integers // Advances in cryptology–eurocrypt 2010: Springer, 2010, p. 24–43.
- [13] C. Gentry. A fully homomorphic encryption scheme, Ph.D. Thesis, (2009).
- [14] P. V Parmar, S. B Padhar, S. N Patel, N. I Bhatt, R. H Jhaveri. Survey of various homomorphic encryption algorithms and schemes // International Journal of Computer Applications, 2014. Vol. 91, no. 8, p. 26-32.
- [15] S. Katok, p-adic Analysis Compared with Real, Mathematics Advanced Study Semesters (Student Mathematical Library, 37) - American Mathematical Society, Providence, RI, 2007
- [16] Zaryab Khan. Quasi-Linear Time Fully Homomorphic Public Key Encryption Algorithm (ZK111) // IJTPC, Vol. 1, November 2012.
- [17] E. Yurova, A. Khrennikov, Criteria of ergodicity for p-adic dynamical systems in terms of coordinate functions. Chaos, Solitons & Fractals, Vol 60, 2014, pp. 11-30
- [18] A. Khrennikov, E. Yurova, Criteria of measure-preserving for p-adic dynamical systems in terms of the van der Put basis. Journal of Number Theory, 133(2) (2013) 484-491.
- [19] E.I. Yurova, On measure-preserving functions over \mathbf{Z}_3 . Ultrametric Analysis, and Applications, 4 (2012) 326-335.
- [20] E.I. Yurova, Van der Put basis and p -adic dynamics, p -Adic Numbers, Ultrametric Analysis, and Applications. 2 (2)(2010) 175–178.
- [21] 2014, E. Yurova Axelsson, On recent results of ergodic property for p-adic dynamical systems, P-Adic Numbers, Ultrametric Analysis, and Applications, Vol 6 (3), pp. 235-257.
- [22] V. Anashin, A. Khrennikov and E. Yurova, T-functions revisited: new criteria for bijectivity/transitivity, Springer US, Designs, Codes and Cryptography, Vol 7 (2014), pp. 383-407.
- [23] D. K. Rappe. Homomorphic cryptosystems and their applications, 2006.

- [24] C. Fontaine, F. Galand. A survey of homomorphic encryption for non-specialists // EURASIP Journal on Information Security, 2007. Vol. 2007.